Joshua B. Cooley (AK#1409065)
Katherine Elsner (AK#1411116)
EHRHARDT, ELSNER & COOLEY
215 Fidalgo Ave, Suite 201
Kenai AK 99611
Phone: (907) 283-2876
Fax: (907) 283-2896
josh@907legal.com
katie@907legal.com

[Additional Counsel Listed on Signature Page]

Attorneys for the Plaintiff and Putative Class

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF ALASKA

MELVIN DENNING, individually and on behalf of all others similarly situated, Plaintiff, v. **FAIRBANKS UROLOGY, LLC**, Defendant.	Case No.: _____ **JURY TRIAL DEMANDED** **CLASS ACTION**

CLASS ACTION COMPLAINT

1. Plaintiff Melvin Denning ("Plaintiff"), individually and on behalf of all others similarly situated, brings this class action lawsuit against Defendant Fairbanks Urology, LLC ("Fairbanks," "Fairbanks Urology," or "Defendant) to obtain damages, restitution, and injunctive relief. Plaintiff makes the following allegations upon information

and belief, except as to his own actions, the investigation of his counsel, and facts that are a matter of public record.

I. NATURE OF THE ACTION

2. This class action arises out of Defendant's failure to properly safeguard and protect Plaintiff's and Class Members' highly sensitive protected health information ("PHI") and/or personally identifiable information ("PII") resulting in a large and preventable data breach that impacted at least **4,289** individuals ("Data Breach" or "Breach").[1] As a result, Plaintiff's and the Class's PHI/PII was compromised and is now in the hands of cybercriminals who can immediately put their PHI/PII to a variety of sordid uses.

3. Fairbanks treats men and women with urinary and sexual symptoms.[2] Some of the medical conditions Fairbanks treats include, erectile dysfunction, penile curvature (Peyronie's disease), penile fracture, prostate enlargement, urinary tract infections, low testosterone, low libido, bladder cancer, atrophic vaginitis, testicular pain, testicular cancer, and infertility.[3] In other words, patients seeking treatment from Fairbanks are often doing so at a very vulnerable time in their lives.

4. In connection with the medical services Fairbanks provides, Fairbanks acquired the highly sensitive PHI of Plaintiff and the Class, including their names, diagnosis/clinical information, doctors' names, medical procedure information, medical

[1] U.S. DEPT. OF HEALTH AND HUMAN SERVICES, *Cases Currently Under Investigation*, *Fairbanks Urology*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (search "Fairbanks Urology").
[2] https://fairbanksurology.com/conditions/.
[3] *Id.*

record numbers, and treatment information.

5. Fairbanks also acquired highly sensitive PII, such as addresses, email addresses, phone numbers, Social Security numbers, health insurance information, and financial information (such as payment card information and account information).

6. On June 13, 2025, Fairbanks learned that an email phishing incident resulted in access to an undisclosed number of email accounts and SharePoint accounts between December 13, 2024, and December 16, 2024.

7. In other words, in direct violation of recognized industry standards and data security best practices, Fairbanks stored the highly sensitive PHI and PII it collected from Plaintiff and the Class on its email accounts and SharePoint accounts.[4]

8. Despite the Breach occurring on or around December 13, 2024, through December 16, 2024, Fairbanks did not discover the Breach until ***six (6) months later***—June 13, 2025.

9. To make matters worse, Fairbanks did not notify victims of the Data Breach of the Breach's occurrence until on or around June 27, 2025.[5]

10. Because the services Fairbanks provides involve highly private and sensitive matters, such as sexual health, the exposure of names, diagnosis/clinical information, doctors' names, medical procedure information, medical record numbers, and treatment information in the Data Breach is particularly egregious and embarrassing for many Class Members and is an extreme invasion privacy.

[4] Exhibit 1 (Plaintiff's Notice of Data Breach Letter).
[5] *Id.*

11. Upon information and belief, the Data Breach was a direct result of Fairbanks's failure to implement adequate and reasonable cybersecurity procedures and protocols necessary to protect individuals' PHI/PII. Indeed, the Data Breach makes it clear that Fairbanks was not adequately protecting the sensitive PHI/PII entrusted to it because it was easily accessible in email and SharePoint accounts.

12. Fairbanks maintained Plaintiff's and the Class's PHI/PII in a reckless manner. Specifically, the PHI/PII was maintained in a condition vulnerable to cyberattacks.

13. Cybercriminals intentionally targeted Fairbanks because of its inadequately secured accounts and because of the highly sensitive information it stores within those accounts. As a result, the PHI/PII of Plaintiff and Class is in the hands of cybercriminals.

14. Upon information and belief, the mechanism of the Data Breach and potential for improper disclosure of Plaintiff's and Class Members' PHI/PII was a known risk to Fairbanks. Fairbanks was on notice that failing to take steps necessary to secure PHI/PII from those risks left the PHI/PII in a dangerous condition.

15. Plaintiff brings this class action lawsuit on behalf of himself, and all others similarly situated to address Defendant's failure to safeguard Plaintiff's and the Class's PHI/PII and for failing to provide adequate and timely of the Data Breach to Plaintiff.

16. Fairbanks disregarded the rights of Plaintiff and Class Members (defined below) by, *inter alia*, intentionally, willfully, recklessly, or negligently failing to take adequate and reasonable measures to ensure its accounts were protected against unauthorized intrusions; failing to disclose that it did not have adequately robust computer systems and security practices to safeguard Plaintiff's and Class Members' PHI/PII; failing

to take standard and reasonably available steps to prevent the Data Breach; and failing to provide Plaintiff and Class Members with prompt and full notice of the Data Breach.

17. In addition, Fairbanks failed to properly monitor the accounts compromised in the Breach. Had Fairbanks properly monitored its accounts, it would have discovered the intrusion sooner rather than allowing cybercriminals days of unfettered access to the PHI of Plaintiff Class Members.

18. Plaintiff's and Class Members' identities are now at risk because of Defendant's negligent conduct because the PHI/PII that Defendant collected and maintained is now in the hands of data thieves.

19. Armed with the PHI/PII stolen in the Data Breach, data thieves can commit a variety of crimes including: (i) filing false medical claims using Class Members' information; (ii) impersonating Class Members to get medical services; (iii) unlawfully receiving Class Members' Medicare or Medicaid benefits; (iv) purchasing prescription medications in Class Members' names; (v) deploying phishing campaigns to trick Class Members into giving them more sensitive information or to pay for fake services they never received; (vi) blackmailing victims; (vii) selling it on the dark web for profit; and (viii) extorting victims for ransom demands.[6]

20. The Data Breach is also a source of embarrassment and humiliation for Plaintiff and Class Members because their private medical diagnoses have been accessed by an unauthorized actor.

[6] https://www.paubox.com/blog/how-hackers-use-stolen-patient-data.

21. As a result of the Data Breach, Plaintiff and Class Members have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiff and Class Members must now and for years into the future closely monitor their medical care, health insurance, and financial accounts to guard against medical and identity theft.

22. Plaintiff and Class Members will also incur out of pocket costs for, *e.g.*, purchasing medical monitoring services, credit monitoring services, credit freezes, credit reports, and/or other protective measures to deter and detect medical and identity theft.

23. Plaintiff seeks to remedy these harms on behalf of himself and all similarly situated individuals whose PHI/PII was accessed and/or acquired during the Data Breach and seek remedies including, but not limited to, compensatory damages, nominal damages, reimbursement of out-of-pocket costs, attorneys' fees and expenses, and injunctive relief including improvements to Fairbanks's data security systems, future annual audits, as well as long-term and adequate medical monitoring services funded by Defendant, and declaratory relief.

II. THE PARTIES

24. Plaintiff **Melvin Denning** is an individual who is domiciled in Ester, AK. Plaintiff is a victim of the Data Breach and received a Notice of Data Breach Letter ("Notice Letter") from Defendant dated June 27, 2025.[7]

25. Defendant **Fairbanks Urology, LLC** is an Alaska limited liability company with its mailing address located at 607 Old Steese Highway, Suite B306, Fairbanks, Alaska

[7] *Id.*

99701-6809. Fairbanks's registered agent is Tony Nimeh, who can be served at the same address. Fairbanks's principal place of business is located at 1211 Cushman Street, Fairbanks, AK 99701.

III. JURISDICTION AND VENUE

26. Jurisdiction is proper in this Court under 28 U.S.C. § 1332 (diversity jurisdiction). Specifically, this Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action where the amount in controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the proposed Class and at least one other Class Member is a citizen of a state different from Defendant.

27. Supplemental jurisdiction to adjudicate issues pertaining to state law is proper in this Court under 28 U.S.C. § 1367.

28. Defendant is headquartered and routinely conducts business in the State where this District is located, has sufficient minimum contacts in this State and has intentionally availed itself of this jurisdiction by marketing and selling products and/or services, and by accepting and processing payments for those products and/or services within this State.

29. Venue is proper in this Court under 28 U.S.C. § 1391 because a substantial part of the events that gave rise to Representative Plaintiffs' claims took place within this District, and Defendant does business in this Judicial District.

IV. FACTUAL ALLEGATIONS

A. Defendant Collected Plaintiff's and the Class's PII/PHI During the Course of the Highly Confidential Services it Provides.

30. Fairbanks Urology is based in Fairbanks, Alaska and provides men and women with urinary and sexual symptoms.[8]

31. The services and procedures Fairbanks provide are of a highly sensitive and confidential nature.[9]

32. The conditions Fairbanks treats includes, but is not limited to:

a) Low testosterone;
b) High Testosterone;
c) Erectile Dysfunction;
d) Penile Curvature (Peyronie's);
e) Penile Fracture;
f) Prostatitis;
g) Testicular Pain;
h) Infertility;
i) Testicular Torsion;
j) Hydrocele;
k) Urethral Stricture;
l) BPH / Prostate Enlargement;
m) IPSS questionnaire;
n) Frequency in Men;
o) Nocturia / Nightime Urination;
p) Urocuff;
q) Cystoscopy;
r) Transrectal Ultrasound;
s) Transurethral Resection (TURP);
t) Greenlight Photovaporization;
u) Button Vaporization;
v) Urolift Procedure;
w) Low Libido in women;
x) Estrogen deficiency;

[8] https://fairbanksurology.com/conditions/.
[9] *Id.*

y) Atrophic Vaginitis;
z) Prostate cancer;
aa) Bladder cancer; and
bb) Testicular cancer.[10]

33. Fairbanks also performs a variety highly personal surgeries, including but not limited to:

a) Vasectomies
b) Penile Prostheses;
c) Circumcisions;
d) Artificial Urinary Sphincters;
e) Bladder Tumor Resections;
f) Mid-Urethral Slings;
g) Urethroplasties; and
h) Robotic Prostatectomies.[11]

34. As evidenced by the above, Fairbanks provides a wide range of highly sensitive and personal medical services to individuals who often have very sensitive and private health conditions that do not want this information to be publicly known nor accessed by unauthorized individuals.

35. In conjunction with the health services Fairbanks provides, Fairbanks collects PHI from the patients it provides services to, including Plaintiff and the Class.

36. Fairbanks also collects and stores the PII of its patients, including their names, addresses, email addresses, phone numbers, Social Security numbers, health insurance information, and financial information (such as payment card information and account information). Upon information and belief, PII was also compromised in the Data Breach.

[10] https://fairbanksurology.com/conditions/.
[11] https://fairbanksurology.com/surgeries/.

37. Plaintiff and the Class entrusted their PHI/PII to Fairbanks with the mutual agreement and understanding that Fairbanks would protect their PHI/PII from unauthorized access.

38. As a healthcare provider who is a covered entity under HIPAA, Fairbanks should have implemented technical, organizational, and physical safeguards designed to protect the PHI and PII it collects. However, Fairbanks failed to take data security seriously, resulting in a Data Breach that exposed Plaintiff's and the Class's PII/PHI.

B. Defendant's Data Breach Exposed the PII/PHI of Plaintiff and the Class.

39. According to Fairbanks, on June 13, 2025, Fairbanks learned that an email phishing incident had resulted in unauthorized access to patient information in an undisclosed number of email accounts and SharePoint accounts.[12]

40. After an investigation, Fairbanks determined that unauthorized parties accessed an undisclosed number of email accounts and SharePoint accounts between December 13, 2024, and December 16, 2024.[13]

41. Fairbanks confirmed that "certain emails and SharePoint files were ***accessed*** by the unauthorized parties."[14]

42. The types of information accessed in the Data Breach, according to the Notice Letter Plaintiff received, included: names, diagnosis/clinical information, doctors' names, medical procedure information, medical record numbers, and treatment

[12] Ex. 1.
[13] *Id.*
[14] *Id.* (emphasis added).

information.

43. Upon information and belief, the following PII was also compromised in the Data Breach: addresses, email addresses, phone numbers, Social Security numbers, health insurance information, and financial information (such as payment card information and account information).

44. A covered entity under HIPAA—such as Fairbanks—must notify the HHS if it discovers a breach of unsecured PHI. *See* 45 C.F.R. § 164.408. On June 27, 2025, Fairbanks reported the Data Breach to the United States Department of Health and Human Services ("HHS"), disclosing that: (i) 4,289 individuals were impacted by the Breach; (ii) the type of the breach was hacking/IT incident; and (iii) the information accessed in the Breach was located on email accounts.[15]

45. Additionally, on or around June 27, 2025—over six (6) months after the Data Breach began—Fairbanks began sending Notice Letters to victims of the Data Breach.[16]

46. In the Notice Letters, Fairbanks failed to explain why it took six (6) months for Fairbanks to learn it had experienced a Data Breach. Fairbanks's failure to timely detect the Data Breach, particularly for a lengthy period of time, is indicative of poor data security infrastructure, procedures, and protocols.

47. After receiving the Notice Letters, it is reasonable for recipients, including Plaintiff and Class Members, to believe that the risk of future harm (including medical and

[15] U.S. DEPT. OF HEALTH AND HUMAN SERVICES, *Cases Currently Under Investigation*, *Fairbanks Urology*, https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf (search "Fairbanks Urology").
[16] *Id.*

identity theft) is substantial and imminent, and that it is necessary for them to take steps to mitigate the substantial risk of impending and future harm.

48. Indeed, Fairbanks admonishes victims of the Data Breach to review statements received from healthcare providers and health insurance plans to determine if there are services on the statements that were not received. [17]

49. Despite stressing in the Notice Letters that Class Members monitor their statements, Fairbanks did not provide any complimentary credit monitoring or medical monitoring to victims of the Breach. In effect, Defendant is shirking its responsibility for the harm and increased risk of identity theft and fraud it has caused Plaintiff and members of the Class.

50. The Breach has placed immense distress and financial burdens on the Data Breach victims.

51. Upon information and belief, cybercriminals intentionally targeted and gained access to Plaintiff's and the Class's PHI/PII with the intent of engaging in misuse of the PHI/PII, including marketing and selling Plaintiff's and Class Members' PHI/PII to fraudsters as that is the *modus operandi* of data thieves.

52. Fairbanks could have prevented the Data Breach—but failed to do so. The perpetrators of the Data Breach managed to gain access to Fairbanks's systems through a widely known method referred to as "phishing."

[17] *Id.*

53. "Phishing is a type of social engineering and cybersecurity attack where the attacker impersonates someone else via email or other electronic communication methods, including social networks and Short Message Service (SMS) text messages, to reveal sensitive information."[18]

54. "Typically, a victim receives a message that appears to have been sent by a known contact or organization. The attack is then carried out either when the victim clicks on a malicious file attachment or clicks on a hyperlink connecting them to a malicious website. In either case, the attacker's objective is to install malware on the user's device or direct them to a fake website. Fake websites are set up to trick victims into divulging personal and financial information, such as passwords, account IDs or credit card details."[19]

55. The Cybersecurity & Infrastructure Security Agency ("CISA"), states "**many security breaches are avoidable if people are trained to spot and avoid phishing messages."[20]**

56. Healthcare entities, such as Defendant, can prevent data breaches perpetrated through phishing by:

> a) **Comprehensive Employee Training and Awareness Programs**: Conduct regular training sessions to educate employees on identifying phishing attempts, including recognizing suspicious emails, links, and attachments. Implement simulated phishing campaigns to test employees' responses and reinforce training. Provide feedback and additional training to those who fall for the simulations. Establish and promote a clear procedure for reporting suspected phishing attempts. Ensure that

[18] https://www.techtarget.com/searchsecurity/definition/phishing.
[19] *Id.*
[20] https://www.cisa.gov/secure-our-world/teach-employees-avoid-phishing.

employees know who to contact and how to report suspicious activity.

b) **Implement Multi-Factor Authentication (MFA)**: Enforce multi-factor authentication for accessing all critical systems and data, reducing the risk of compromised credentials being used for unauthorized access. Use dynamic and context-aware authentication methods that adapt based on the user's location, device, and behavior.

c) **Email and Domain Security Measures**: Implement DMARC, along with SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail), to protect your domain from being used in phishing attacks. Set up advanced email filtering rules to automatically flag or quarantine emails that contain common phishing indicators, such as spoofed addresses or suspicious attachments.

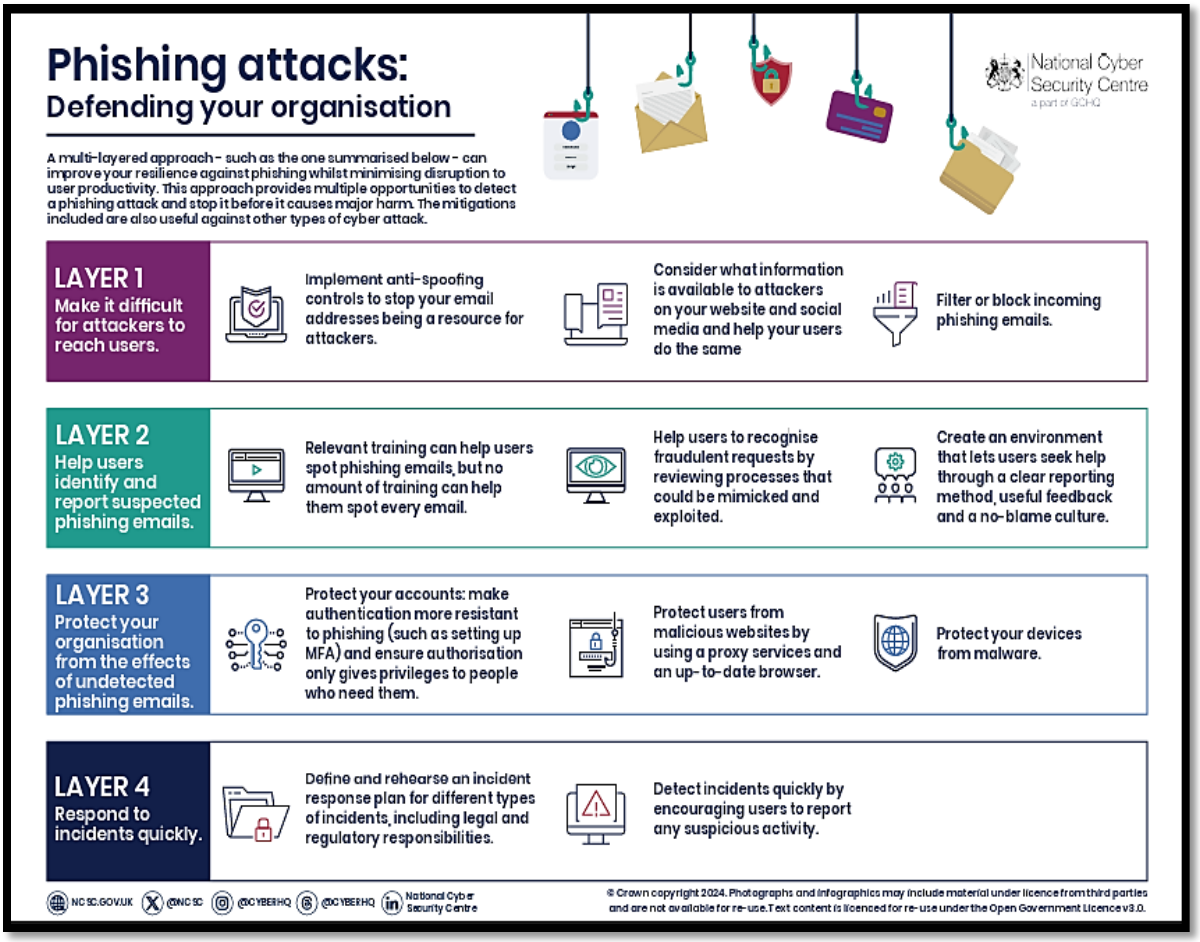
d) **Strengthen Access Controls and Permissions**: Implement the principle of least privilege, ensuring that employees only have access to the information and systems necessary for their job functions. This reduces the risk of phishing attacks gaining access to critical systems. Conduct regular audits of user access rights to ensure compliance with access control policies and to identify and revoke unnecessary permissions.

e) **Establish Incident Response and Recovery Plans**: Develop and regularly update an incident response plan that outlines the steps to be taken in the event of a phishing attack. Ensure all employees are aware of the plan and their roles within it. Have robust data backup and recovery procedures in place. Regularly test these procedures to ensure that data can be restored quickly and accurately in case of an attack. Conduct a thorough analysis after any phishing incident to understand how it happened, assess the impact, and implement measures to prevent future attacks.[21]

57. Defendant could have and should have implemented the following layers of protection recommended by the National Cyber Security Centre:[22]

[21] https://perception-point.io/guides/phishing/how-to-prevent-phishing-attacks/#:~:text=TIPS%20FROM%20THE%20EXPERT,location%2C%20device%2C%20and%20behavior.

[22] https://www.ncsc.gov.uk/guidance/phishing.



58. Additionally, Encryption at rest for sensitive data, such as the PHI/PII at issue here, is a non-negotiable security measure. However, Fairbanks failed to utilize such encryption. Had Fairbanks used such encryption the Data Breach would have never occurred.

C. Cybercriminals Will Use Plaintiff's and Class Members' PHI/PII to Defraud Them.

59. PHI/PII is of great value to hackers and cybercriminals, and the data accessed and/or acquired in the Data Breach can and will be used in a variety of ways by criminals to exploit Plaintiff and Class Members and to profit off their misfortune.

60. Hackers want stolen medical records to commit identity theft, use the stolen

data as a ransom, sell it on the dark web or impersonate the victim to receive medical services. Medical records are valuable to cybercriminals as they allow cybercriminals to commit fraud and go undetected longer than they can with other personally identifiable information.[23]

61. Gary Cantrell, head of investigations at the HHS Office of Inspector General, said hackers tend to steal medical records because they are "a treasure trove of [] information about you." They contain a patient's full name, address history, financial information, and social security numbers—which is enough information for hackers to take out a loan or set up a line of credit under patients' names, according to *Computerworld*.[24]

62. For example, with the PHI stolen in the Data Breach, bad actors can: (i) use the stolen PHI to visit a doctor (during an emergency, this false information could prevent the victim from receiving the treatment they need, or cause the doctor to prescribe the wrong treatment); (ii) file fraudulent insurance claims; (iii) obtain prescription drugs for the purpose of selling them on the black market; (iv) rack up large hospital bills in the victim's name, which may negatively impact the victim's credit; (v) employ phishing tactics using calls, emails or other messages that appear legitimate — to trick victims into giving up more information; and (vi) receive Medicaid or Medicare benefits in the victim's

[23] https://www.keepersecurity.com/blog/2024/01/11/why-do-hackers-want-medical-records/#:~:text=Hackers%20want%20stolen%20medical%20records,victim%20to%20receive%20medical%20services.
[24] https://www.advisory.com/daily-briefing/2019/03/01/hackers.

name.[25]

63. But increasingly, hackers are selling medical information for profit on the black market.[26] According to Reuters, buyers might use the information to create fake IDs to purchase medical equipment or drugs, or to file a false insurance claim.[27]

64. These criminal activities have and will result in devastating financial and personal losses to Plaintiff and Class Members.

65. Medical-related identity theft is one of the most common, most expensive, and most difficult to prevent forms of identity theft. According to Kaiser Health News, "medical-related identity theft accounted for 43 percent of all identity thefts reported in the United States in 2013[,]" which is more than identity thefts involving banking and finance, the government and the military, or education.[28]

66. When cybercriminals manage to steal PHI—as they did here—there is no limit to the amount of fraud to which Plaintiff and Class Members are exposed.

67. PHI is such a valuable commodity to identity thieves that once it has been compromised, criminals will use it for years.[29]

68. The Data Breach at issue here was targeted and financially motivated, as the

[25] https://www.idwatchdog.com/education/what-is-medical-identity-theft#:~:text=What%20can%20a%20criminal%20do,or%20purchase%20costly%20medical%20services; https://www.equifax.com/personal/education/identity-theft/articles/-/learn/medical-identity-theft/.
[26] https://www.advisory.com/daily-briefing/2019/03/01/hackers.
[27] *Id.*
[28] Michael Ollove, *The Rise of Medical Identity Theft in Healthcare*, KAISER HEALTH NEWS (Feb. 7, 2014), https://khn.org/news/rise-of-indentity-theft/.
[29] *Id.*

only reason cybercriminals go through the trouble of hacking companies like Fairbanks is to steal the highly sensitive PII/PHI they maintain, which can be exploited and sold for use in the kinds of criminal activity described herein.

69. "Medical records are a gold mine for criminals—they can access a patient's name, DOB, Social Security and insurance numbers, and even financial information all in one place."[30] A complete identity theft kit that includes health insurance credentials may be worth up to $1,000 on the black market.[31]

70. According to Experian, a patient's full medical records can sell for up to $1,000. By comparison, Social Security numbers and credit card information usually sell for $1 and up to $110, respectively.[32]

71. A Social Security number, date of birth, and full name can sell for $60 to $80 on the digital black market.[33]

72. It is evident PHI is even more valuable on the black market than PII.[34]

73. According to the Center for Internet Security, "[t]he average cost of a data breach incurred by a non-healthcare related agency, per stolen record, is $158. For healthcare agencies the cost is an average of $355. Credit card information and PII sell for

---

[30] *You Got It, They Want It: Criminals Targeting Your Private Healthcare Data, New Ponemon Study Shows*, IDX (May 14, 2015) https://www.idx.us/knowledge-center/you-got-it-they-want-it-criminals-are-targeting-your-private-healthcare-dat..

[31] *Managing cyber risks in an interconnected world: Key findings from The Global State of Information Security Survey 2015*, PRICEWATERHOUSECOOPERS (Sept. 30, 2014), https://www.pwc.com/gx/en/consulting-services/information-security-survey/assets/the-global-state-of-information-security-survey-2015.pdf.

[32] https://www.advisory.com/daily-briefing/2019/03/01/hackers

[33] Michael Kan, *Here's How Much Your Identity Goes for on the Dark Web*, PGMAG (Nov. 15, 2017), https://www.pcmag.com/news/heres-how-much-your-identity-goes-for-on-the-dark-web.

[34] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector.

$1-$2 on the black market, but PHI can sell for as much as $363 according to the Infosec Institute. This is because one's personal health history, including ailments, illnesses, surgeries, etc., can't be changed, unlike credit card information or Social Security Numbers."[35]

74. "PHI is valuable because criminals can use it to target victims with frauds and scams that take advantage of the victim's medical conditions or victim settlements. It can also be used to create fake insurance claims, allowing for the purchase and resale of medical equipment. Some criminals use PHI to illegally gain access to prescriptions for their own use or resale."[36]

75. Identity theft experts advise victims of data breaches: "[I]f there is reason to believe that your personal information has been stolen, you should assume that it can end up for sale on the dark web."[37]

76. Hackers may not use the information right away, but this does not mean it will not be used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [I]n some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information **may continue for years**. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[38]

---

[35] *Id.*
[36] *Id.*
[37] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[38] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown*, GAO (July 5, 2007), https://www.gao.gov/products/gao-07-737 (emphasis added).

77. For instance, with a stolen Social Security number, which Plaintiff reasonably believes was also stolen in the Data Breach, criminals can open financial accounts, get medical care, file fraudulent tax returns, commit crimes, and steal benefits.[39]

78. Identity theft victims must spend countless hours and large amounts of money repairing the impact to their credit as well as protecting themselves in the future.[40]

79. Defendant made no offering of identity monitoring or medical monitoring to Plaintiff and the Class. Plaintiff and the Class are left unprotected from Fairbanks's negligent failure to secure and protect their PHI/PII.

80. The unfortunate truth is the full scope of the harm has yet to be realized. There may be a time lag between when harm occurs and when it is discovered, and also between when PHI/PII is stolen and when it is used.

81. Plaintiff and Class Members will need to pay for their own medical monitoring and credit monitoring for the rest of their lives due to Defendant's negligence.

82. Furthermore, identity and medical monitoring services only alert someone to the fact that they have already been the victim of identity or medical theft—it does not prevent identity or medical theft.[41]

83. Nor can identity monitoring service or a medical monitoring services remove

---

[39] *See* Nikkita Walker, *What Can Someone Do with Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), https://blog.credit.com/2017/11/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[40] *Guide for Assisting Identity Theft Victims*, FEDERAL TRADE COMMISSION (Sept. 2013), https://www.global-screeningsolutions.com/Guide-for-Assisting-ID-Theft-Victims.pdf.

[41] *See* Kayleigh Kulp, *Credit monitoring services may not be worth the cost*, CNBC (Nov. 30, 2017, 9:00 AM), https://www.cnbc.com/2017/11/29/credit-monitoring-services-may-not-be-worth-the-cost.html.

PHI/PII from the dark web.[42]

84. "The people who trade in stolen personal information [on the dark web] won't cooperate with an identity theft service or anyone else, so it's impossible to get the information removed, stop its sale, or prevent someone who buys it from using it."[43]

85. As a direct and proximate result of the Data Breach, Plaintiff and the Class have been damaged and placed at an imminent and continuing increased risk of harm from fraud and identity theft. Plaintiff and the Class must now take the time and effort to mitigate the actual and potential impact of the Data Breach on their everyday lives, including placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, reviewing their explanation of benefits statements, reviewing medical statements, closing or modifying financial accounts, and closely reviewing and monitoring bank accounts, credit reports, and medical records for unauthorized activity for years to come.

86. Even more serious is the identity restoration that Plaintiff and other Class Members must go through, which can require spending countless hours filing police reports, filling out IRS forms, completing Federal Trade Commission checklists and Department of Motor Vehicle driver's license replacement applications, and calling financial institutions to cancel fraudulent credit applications, to name just a few of the steps Plaintiff and the Class must take.

[42] *Dark Web Monitoring: What You Should Know*, CONSUMER FEDERATION OF AMERICA (Mar. 19, 2019), https://consumerfed.org/consumer_info/dark-web-monitoring-what-you-should-know/.
[43] *Id.*

87. Plaintiff and the Class have or will experience the following concrete and particularized harms for which they are entitled to compensation, including:

a. Actual identity theft;

b. Trespass, damage to, and theft of their personal property, including their PHI/PII;

c. Improper disclosure and theft of their PHI/PII;

d. The imminent and certainly impending injury flowing from potential fraud and identity theft posed by their PHI/PII being placed in the hands of criminals;

e. Loss of privacy suffered as a result of the Data Breach, including the harm of knowing cybercriminals have their PHI/PII;

f. Ascertainable losses in the form of time taken to respond to identity theft and medical fraud, including lost opportunities and lost wages from uncompensated time off from work;

g. Ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably expended to remedy or mitigate the effects of the Data Breach;

h. Ascertainable losses in the form of diminution of the value of Plaintiff's and Class Members' PHI/PII, for which there is a well-established and quantifiable national and international market;

i. The loss of use of and access to their credit, accounts, medical records, and/or funds;

j. Damage to their credit due to fraudulent use of their PHI/PII; and/or

k. Increased cost of borrowing, insurance, deposits, and the inability to secure more favorable interest rates because of a reduced credit score.

88. Moreover, Plaintiff and Class Members have an interest in ensuring that their PHI/PII, which remains in the possession of Fairbanks, is protected from further breaches through the implementation of industry standard security measures and safeguards. Fairbanks has shown itself wholly incapable of protecting Plaintiff's and Class Members' PHI/PII.

89. Plaintiff and Class Members also have an interest in ensuring that their PHI/PII is removed from all Defendant's servers, systems, and files.

90. The notice provided by Fairbanks acknowledged that the Data Breach would cause harm to affected individuals and that financial harm would likely occur.[44]

91. At Defendant's suggestion, Plaintiff is desperately trying to mitigate the damages Defendant caused him.

92. Given the kind of PHI/PII Defendant made accessible to hackers, however, Plaintiff is certain to incur additional damages. Because thieves have their PHI/PII, Plaintiff and Class Members will need to have identity theft monitoring and medical monitoring for the rest of their lives. Some may even need to go through the long and arduous process of getting a new Social Security number, with all the loss of credit and

[44] Ex. 1.

employment difficulties that come with a new number.[45]

93. None of this should have happened because the Data Breach was entirely preventable.

D. Defendant was Aware of the Risk of Data Breaches.

94. According to the Center for Internet Security, "the health industry experiences more data breaches than any other sector."[46] This is because "Personal Health Information (PHI) is more valuable on the black market than credit card credentials or regular Personally Identifiable Information (PII). Therefore, there is a higher incentive for cyber criminals to target medical databases. They can sell the PHI and/or use it for their own personal gain."[47]

95. "In 2023, more than 540 organizations and 112 million individuals were implicated in healthcare data breaches reported to the HHS Office for Civil Rights (OCR), compared to 590 organizations and 48.6 million impacted individuals in 2022."[48]

96. "The number of cybersecurity attacks disrupting the healthcare sector has continued to be a growing concern. In the last three years, more than 90% of all healthcare organizations have reported at least one security breach which can manifest in denial of service, malicious code, ransomed data, and more."[49]

---

[45] *What happens if I change my Social Security number?*, LEXINGTON LAW (Aug. 10, 2022), https://www.lexingtonlaw.com/blog/credit-101/will-a-new-social-security-number-affect-your-credit.html.
[46] *Data Breaches: In the Healthcare Sector*, CENTER FOR INTERNET SECURITY, https://www.cisecurity.org/insights/blog/data-breaches-in-the-healthcare-sector.
[47] *Id.*
[48] *This Year's Largest Healthcare Data Breaches*, HEALTH IT SECURITY (Dec. 26, 2023), https://healthitsecurity.com/features/this-years-largest-healthcare-data-breaches.
[49] *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html.

97. "Healthcare organi[z]ations are rich targets for cybercriminals because they hold a large amount of sensitive patient data. This data can be used to commit identity theft or fraud or sold on the black market. Hackers can access this data in many ways, including phishing emails, malware, and unsecured networks."[50]

98. It is no secret that "[h]ealthcare data breaches are reaching record highs. Indeed, healthcare now sees more cyberattacks than any other industry. Fully one-third of all cyberattacks are aimed at healthcare institutions. Why? Because healthcare is a valuable and vulnerable target. Hospitals and healthcare institutions are a prime target for cybercrime due to the vast amount of sensitive data they hold."[51]

99. The health industry is frequently recognized as one of the most vulnerable industries for a cyberattack.[52]

100. Defendant should have been aware, and indeed was aware, that it was at risk of a data breach that could expose the PHI that it solicited, collected, stored, and maintained, especially given the rise in data breaches.

101. Defendant was aware of the risks and harm that could result from inadequate data security but threw caution to the wind.

---

[50] Troy Beamer, *What Industries Are Most Vulnerable to Cyber Attacks In 2024?*, TECHNEWS (Feb. 27, 2024), https://www.techbusinessnews.com.au/what-industries-are-most-vulnerable-to-cyberattacks-in-2022/.

[51] *What Industries Are Most Vulnerable to Cyberattacks?*, PSM, https://www.psmpartners.com/blog/most-targeted-industries-for-cyber-attacks/.

[52] *See, e.g.*, *id.*; Liudmyla Pryimenko, *The 7 Industries Most Vulnerable to Cyberattacks*, EKRAN (Mar. 25, 2024), https://www.ekransystem.com/en/blog/5-industries-most-risk-of-data-breaches; Ani Petrosyan, *Distribution of cyberattacks across worldwide industries in 2023*, STATISTA (Mar. 22, 2024), https://www.statista.com/statistics/1315805/cyber-attacks-top-industries-worldwide/; *6 Industries Most Vulnerable to Cyber Attacks*, WGU (Aug. 3, 2021), https://www.wgu.edu/blog/6-industries-most-vulnerable-cyber-attacks2108.html.

E. Fairbanks Could Have Prevented the Data Breach.

102. Data breaches are preventable.[53] "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions."[54] "Organizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised[.]"[55]

103. Most reported data breaches "are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and disciplined manner so that a *data breach never occurs*."[56]

104. Here, many failures laid the groundwork for the Data Breach.

105. The FTC has published guidelines that establish reasonable data security practices for businesses.[57]

106. The FTC guidelines emphasize the importance of having a data security plan, regularly assessing risks to computer systems, and implementing safeguards to control such risks.[58]

107. The FTC guidelines establish that businesses should protect the confidential

---

[53] Lucy L. Thomson, *Despite the Alarming Trends, Data Breaches Are Preventable*, DATA BREACH AND ENCRYPTION HANDBOOK (Lucy Thompson, ed., 2012), available at https://lawcat.berkeley.edu/record/394088.
[54] *Id.* at 17.
[55] *Id.* at 28.
[56] *Id.*
[57] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), available at https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[58] *Id.*

information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies for installing vendor-approved patches to correct security problems.[59]

108. The FTC guidelines also recommend that businesses utilize an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating hacking attempts; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[60]

109. According to information and belief, Fairbanks failed to follow reasonable and necessary industry standards to prevent a data breach, including the FTC's guidelines.

110. Upon information and belief, Fairbanks also failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework, NIST Special Publications 800-53, 53A, or 800-171; the Federal Risk and Authorization Management Program (FEDRAMP); or the Center for Internet Security's Critical Security Controls (CIS CSC), which are well respected authorities in cybersecurity readiness.

111. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[61]

112. To prevent and detect the Breach, Fairbanks could and should have taken, as

[59] *Id.*
[60] *Id.*
[61] *See How to Protect Your Networks from RANSOMWARE*, at 3, available at https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

recommended by the Federal Bureau of Investigation, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.
- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share

permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Used application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[62]

113. According to information and belief, Fairbanks failed to do any of the above.

114. Further, Fairbanks could and should have taken the following measures:

[62] *Id.* at 3–4.

- **Update and patch your computer**. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks.
- **Use caution with links and when entering website addresses**. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net).
- **Open email attachments with caution**. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe**. Check a website's security to ensure the information you submit is encrypted before you provide it.
- **Verify email senders**. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the

sender is authentic before you contact them.

- **Inform yourself**. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs**. Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic.[63]

115. In addition, Defendant could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Harden internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audits

Thoroughly investigate and remediate alerts.

- Prioritize and treat commodity malware infections as potential full compromise of the system

[63] *See Protecting Against Ransomware*, CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY (revised Sept. 2, 2021), https://www.cisa.gov/news-events/news/protecting-against-ransomware (internal citations omitted).

Include IT professionals in security discussions.

- Ensure collaboration among security operations, security administrators, and information technology administrators to configure servers and other endpoints securely

Build and maintain credential hygiene

- Use multifactor authentication or network level authentication and enforce strong, randomized, just-in-time local administrator passwords

Apply principle of least-privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

Harden infrastructure

- Utilize Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and Antimalware Scan Interface for Office Visual Basic for Applications[64]

116. Given that Fairbanks was storing the PHI/PII of thousands of individuals,

[64] *See Human-operated ransomware attacks: A preventable disaster*, MICROSOFT THREAT INTELLIGENCE (Mar 5, 2020), https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/.

Fairbanks could and should have implemented all of the above measures to prevent and detect cyberattacks.

117. Specifically, among other failures, Fairbanks had far too much confidential unencrypted PII/PHI held on its systems. Such PHI/PII should have been segregated into an encrypted system.[65]

118. Moreover, it is well-established industry standard practice for a business to dispose of confidential PHI/PII once it is no longer needed.[66]

119. The FTC has repeatedly emphasized the importance of disposing of unnecessary PHI/PII: "Keep sensitive data in your system only as long as you have a business reason to have it. Once that business need is over, properly dispose of it. If it's not on your system, it can't be stolen by hackers."[67] Rather than following this basic standard of care, Fairbanks kept thousands of individuals' unencrypted PHI on their inadequately secured systems indefinitely.

120. In sum, the Data Breach could have been easily prevented through standard practices like the use of industry standard network segmentation and encryption of all PHI/PII—which Fairbanks negligently failed to do.

121. Further, the scope of the Data Breach could have been dramatically reduced had Defendant utilized proper record retention and destruction practices—but Defendant

---

[65] *See* Adnan Raja, *How to Safeguard Your Business Data With Encryption*, DATAINSIDER (Aug. 14, 2018), https://digitalguardian.com/blog/how-safeguard-your-business-data-encryption.
[66] *See Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (Oct. 2016), https://www.ftc.gov/business-guidance/resources/protecting-personal-information-guide-business.
[67] *Id.* at 6.

negligently did no such thing.

F. Defendant had an Obligation to Protect PHI/PII Under the Law and the Applicable Standard of Care.

122. As a healthcare provider handling PHI, Fairbanks is a covered entity under HIPAA (45 C.F.R. § 160.103). As such, Fairbanks is required to comply with the HIPAA Privacy Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), and the HIPAA Security Rule, 45 C.F.R. Part 160 and Part 164, Subparts A and C ("Security Standards for the Protection of Electronic Protected Health Information").

123. HIPAA's Privacy Rule establishes national standards for protecting health information, including health information that is kept or transferred in electronic form.

124. HIPAA's Privacy Rule allows covered entities to disclose PHI to "business associates" if the covered entity obtains satisfactory assurances that the business associate will use the information only for the purposes for which it was engaged by the covered entity, will safeguard the information from misuse, and will help the covered entity comply with some of the covered entity's duties under the Privacy Rule. The satisfactory assurances must be in writing, whether in the form of a contract or other agreement between the covered entity and the business associate.

125. A covered entity's contract or other written arrangement with its business associate must contain the elements specified at 45 CFR 164.504(e). For example, the contract must: (i) describe the permitted and required uses of protected health information by the business associate; (ii) provide that the business associate will not use or further

disclose the PHI other than as permitted or required by the contract or as required by law; and (iii) require the business associate to use appropriate safeguards to prevent a use or disclosure of the protected health information other than as provided for by the contract.

126. Where a covered entity knows of a material breach or violation by the business associate of the contract or agreement, the covered entity is required to take reasonable steps to cure the breach or end the violation, and if such steps are unsuccessful, to terminate the contract or arrangement. If termination of the contract or agreement is not feasible, a covered entity is required to report the problem to the Department of Health and Human Services (HHS) Office for Civil Rights (OCR).

127. Defendant was required to "comply with the applicable standards, implementation specifications, and requirements" of HIPAA "with respect to electronic protected health information." 45 C.F.R. § 164.302.

128. "Electronic protected health information" is "individually identifiable health information . . . that is: (i) transmitted by electronic media; [or] (ii) maintained in electronic media[.]" 45 C.F.R. § 160.103.

129. The HIPAA Security Rule, 45 C.F.R. Part 164, Subpart C, requires Defendant to:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information it or any business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information; and

d. Ensure compliance by its workforce.

130. HIPAA also requires Defendant to "review and modify the security measures implemented . . . as needed to continue provision of reasonable and appropriate protection of electronic protected health information[.]" 45 C.F.R. § 164.306(e).

131. Additionally, HIPAA requires Defendant to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights[.]" 45 C.F.R. § 164.312(a)(1).

132. The HIPAA Breach Notification Rule, 45 C.F.R. §§ 164.400-414, further requires Defendant to provide notice of the Data Breach to each affected individual "without unreasonable delay and in no case later than 60 days following discovery of [the] breach[.]"

133. Fairbanks was also prohibited by the Federal Trade Commission Act, 15 U.S.C. § 45 (the "FTC Act"), from engaging in "unfair or deceptive acts or practices in or affecting commerce[.]" The FTC has concluded that a company's failure to maintain reasonable and appropriate data security for consumers' sensitive personal information is an "unfair practice" in violation of the FTC Act. *See, e.g.*, *FTC v. Wyndham Worldwide Corp.*, 799 F.3d 236 (3d Cir. 2015).

134. Defendant is further required by various states' laws and regulations to protect Plaintiff's and Class Members' PHI/PII.

135. Fairbanks owed a duty to Plaintiff and the Class to design, maintain, and test its computer systems and servers to ensure that the PHI/PII in its possession and control was adequately secured and protected.

136. Fairbanks owed a duty to Plaintiff and the Class to create and implement reasonable data security practices and procedures to protect the PHI/PII in its possession, including adequately training its employees (and any others who accessed PHI/PII within its computer systems) on how to adequately protect PHI/PII.

137. Fairbanks owed a duty to Plaintiff and the Class to implement processes that would detect a breach of its data security systems in a timely manner.

138. Fairbanks owed a duty to Plaintiff and the Class to act upon data security warnings and alerts in a timely fashion.

139. Fairbanks owed a duty to Plaintiff and the Class to disclose if its computer systems and data security practices were inadequate to safeguard individuals' PHI/PII from theft because such an inadequacy would be a material fact in individuals' decisions to entrust Defendant with their PHI/PII.

140. Defendant owed a duty to Plaintiff and the Class to disclose in a timely and accurate manner when data breaches occurred.

141. Defendant owed a duty of care to Plaintiff and the Class because they were foreseeable and probable victims of any inadequate data security practices.

G. Plaintiff's Individual Experience.

142. Plaintiff Denning entrusted his PHI/PII to Fairbanks as a patient with the reasonable expectation and mutual understanding that Defendant would keep his PHI/PII

secure from unauthorized access.

143. By soliciting and accepting Plaintiff Denning's PHI/PII, Defendant agreed to safeguard and protect it from unauthorized access and delete it after a reasonable time.

144. Defendant was in possession of Plaintiff Denning's PHI/PII before, during, and after the Data Breach.

145. Plaintiff Denning received a Notice Letter from Fairbanks, notifying him that an unauthorized party gained access to Fairbanks's accounts and accessed his PHI/PII.[68]

146. Following the Data Breach, Plaintiff Denning made reasonable efforts to mitigate the impact of the Data Breach, including, but not limited to researching the Data Breach, reviewing and monitoring his accounts for fraudulent activity, and/or reviewing his credit reports. Plaintiff Denning estimates he has already spent hours responding to the fallout of the Data Breach.

147. Plaintiff Denning will be forced to expend additional time to review his credit reports, review his medical statements, and monitor his accounts for the rest of his life. This is time, spent at Fairbanks's direction, which has been lost forever and cannot be recaptured.

148. Plaintiff Denning places significant value in the security of his PHI/PII and does not readily disclose it. Plaintiff Denning entrusted Defendant with his PHI/PII with the understanding that Defendant would keep his information secure and would employ

[68] Ex. 1.

reasonable and adequate data security measures to ensure that his PHI/PII would not be compromised.

149. Plaintiff Denning has never knowingly transmitted unencrypted PHI/PII over the internet or any other unsecured source.

150. As a direct and traceable result of the Data Breach, Plaintiff Denning suffered actual injury and damages after his PHI/PII was compromised in the Data Breach, including, but not limited to: (a) lost time and money related to monitoring his accounts, medical statements, and/or credit reports for fraudulent activity; (b) loss of privacy due to his PHI/PII being accessed and stolen by cybercriminals; (c) loss of the benefit of his bargain because Defendant did not adequately protect his PHI/PII; (d) emotional distress because identity thieves now possess his highly confidential and sensitive PHI/PII; (e) imminent and impending injury arising from the increased risk of fraud and identity theft now that his PHI/PII has been stolen and likely published on the dark web; (f) diminution in the value of his PHI/PII, a form of intangible property that Defendant obtained from Plaintiff Denning; and (g) other economic and non-economic harm.

151. Plaintiff Denning has been and will continue to be at a heightened and substantial risk of future identity theft and its attendant damages for ***years*** to come. This risk is certainly real and impending, and is not speculative, given the highly sensitive nature of the PHI/PII stolen in the Data Breach.[69]

[69] *Id.*

152. Knowing that thieves intentionally targeted and stole his PHI/PII and knowing that his PHI/PII is now in the hands of cybercriminals has caused Plaintiff Denning great anxiety beyond mere worry.

153. Plaintiff Denning has a continuing interest in ensuring that his PHI/PII, which, upon information and belief, remains in the possession of Defendant, is protected and safeguarded from future data breaches. Absent Court intervention, Plaintiff Denning's PHI/PII will be wholly unprotected and at-risk of future data breaches.

V. CLASS ACTION ALLEGATIONS

154. Plaintiff incorporates by reference all preceding factual paragraphs as if fully restated here.

155. Plaintiff brings this action against Defendant on behalf of himself, and all other individuals similarly situated. Plaintiff asserts all claims on behalf of a nationwide class (the "Class") defined as follows:

> **All persons who received a Notice Letter from Fairbanks Urology, LLC, informing them that their PHI and/or PII was potentially compromised in the Data Breach.**

156. Excluded from the Class is Defendant, any entity in which Defendant has a controlling interest, and Defendant's officers, directors, legal representatives, successors, subsidiaries, and assigns. Also excluded from the Class is any judge, justice, or judicial officer presiding over this matter and members of their immediate families and their judicial staff members.

157. Plaintiff reserves the right to amend or modify the above Class definition or to propose subclasses in subsequent pleadings and motions for class certification.

158. Plaintiff anticipates the issuance of notice setting forth the subject and nature of the instant action to the proposed Class. Upon information and belief, Defendant's own business records or electronic media can be utilized for the notice process.

159. **Numerosity:** The proposed Class is so numerous that joinder of all members is impracticable. The total number of individuals affected is more than 4,000.

160. **Typicality:** Plaintiff's claims are typical of the claims of the Class because Plaintiff's PHI/PII, like that of every other Class Member, was compromised in the Data Breach. Plaintiff and all members of the Class were injured by the same wrongful acts, practices, and omissions committed by Defendant, as described herein. Plaintiff's claims therefore arise from the same practices or course of conduct that gives rise to the claims of all Class Members.

161. **Adequacy:** Plaintiff is an adequate representative of the Class because Plaintiff's interests do not conflict with the interests of the Class. Plaintiff has retained counsel competent and highly experienced in data breach class action litigation, and Plaintiff and Plaintiff's counsel intend to prosecute this action vigorously. The interests of the Class will be fairly and adequately protected by Plaintiff and his counsel.

162. **Superiority:** A class action is superior to other available means of fair and efficient adjudication of the claims of Plaintiff and the Class. The injury suffered by each individual Class Member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for individual members of the Class to effectively redress Defendant's wrongdoing. Even if Class Members could afford such individual litigation, the court

system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

163. **Commonality and Predominance:** Defendant engaged in a common course of conduct toward Plaintiff and Class Members, in that Plaintiff's and Class Members' PHI/PII was stored on the same network and unlawfully accessed in the same way. There are many questions of law and fact common to the claims of Plaintiff and the other members of the Class, and those questions predominate over any questions that may affect individual members of the Class. Common questions for the Class include:

a. Whether Defendant engaged in the wrongful conduct alleged herein;

b. Whether Defendant owed a duty to Plaintiff and Class Members to adequately protect their PHI/PII;

c. Whether Defendant breached its duty to Plaintiff and Class Members to adequately protect their PHI/PII;

d. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

e. Whether Fairbanks's data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

f. Whether Fairbanks's data security systems prior to and during the Data Breach were consistent with industry standards;

g. Whether Fairbanks knew or should have known that its computer and network security systems, or the computer and network security systems of its vendors, were vulnerable to cyberattacks;

h. Whether Fairbanks's conduct, including its failure to act, resulted in or was the proximate cause of the Data Breach;

i. Whether Fairbanks was negligent in permitting unencrypted PHI/PII belonging to thousands of individuals to be stored within its network;

j. Whether Fairbanks was negligent in failing to adhere to reasonable data retention policies;

k. Whether Defendant breached implied contractual duties to Plaintiff and the Class to use reasonable care in protecting their PHI/PII;

l. Whether Defendant was unjustly enriched by unlawfully retaining a benefit conferred upon it by Plaintiff and Class Members;

m. Whether Fairbanks should have discovered the Data Breach sooner;

n. Whether Defendant failed to adequately respond to the Data Breach, including failing to investigate it diligently and notify affected individuals in the most expedient time possible and without unreasonable delay, and whether this caused damages to Plaintiff and the Class;

o. Whether Defendant continue to breach duties owed to Plaintiff and the Class;

p. Whether Plaintiff and the Class suffered injuries as a proximate result of

Defendant's negligent actions or failures to act;

q. Whether Fairbanks was negligent in selecting, supervising, and/or monitoring Fairbanks;

r. Whether Plaintiff and the Class are entitled to recover damages, equitable relief, and other relief; and

s. Whether Defendant's actions alleged herein constitute gross negligence, and whether Plaintiff and Class Members are entitled to punitive damages.

164. Defendant has acted on grounds that apply generally to the Class as a whole, so that Class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class wide basis.

165. Finally, all members of the proposed Class are readily ascertainable. Defendant has access to Class Members' names and addresses. Class Members have already been preliminarily identified and sent notice of the Data Breach from Fairbanks.

VI. CAUSES OF ACTION

FIRST CAUSE OF ACTION
NEGLIGENCE
(Alleged Against Fairbanks on Behalf of Plaintiff and the Class)

166. Plaintiff re-alleges and incorporates by reference all preceding paragraphs as though fully set forth herein.

167. Fairbanks solicited, collected, stored, and maintained the PHI/PII of Plaintiff and Class Members on inadequately secured computer systems and networks.

168. Upon accepting and storing Plaintiff's and Class Members' PHI/PII on its computer systems and networks, Fairbanks undertook and owed a duty to Plaintiff and

Class Members to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting their PHI/PII from unauthorized access and disclosure.

169. Fairbanks owed a duty of care to Plaintiff and Class Members to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its computer systems and networks, and the personnel responsible for them, adequately protected the PHI/PII.

170. Fairbanks's duty included a responsibility to implement processes by which it could detect a breach of its security systems in a reasonably expeditious period of time and to give prompt notice to those affected in the case of a data breach.

171. Fairbanks had full knowledge of the sensitivity of the PHI/PII in its possession and the types of harm that Plaintiff and Class Members could and would suffer if the PHI/PII was wrongfully accessed or disclosed. Plaintiff and Class Members were therefore the foreseeable victims of any inadequate data security practices.

172. Fairbanks's duty to implement and maintain reasonable data security practices arose as a result of the special relationship that exists between Fairbanks and consumers, which is recognized by laws and regulations, including, but not limited to, HIPAA, the FTC Act, and common law.

173. Fairbanks was in a superior position to ensure its data security practices were sufficient to protect against the foreseeable risk of harm to Plaintiff and Class Members from a data breach.

174. Fairbanks knew Plaintiff and Class Members relied on it to protect their PHI/PII. Plaintiff and Class Members were not in a position to assess the data security

practices used by Fairbanks. Because they had no means to identify Fairbanks's security deficiencies, Plaintiff and Class Members had no opportunity to safeguard their PHI/PII from cybercriminals. Fairbanks exercised control over the PHI/PII stored on its systems and networks; accordingly, Fairbanks was best positioned and most capable of preventing the harms caused by the Data Breach.

175. Fairbanks was aware, or should have been aware, of the fact that cybercriminals routinely target healthcare entities, through cyberattacks in an attempt to steal valuable PHI/PII. In other words, Fairbanks knew of a foreseeable risk to its data security systems but failed to implement reasonable security measures.

176. Fairbanks owed Plaintiff and Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing their PHI/PII, including taking action to reasonably safeguard or delete such data and providing notification to Plaintiff and Class Members of any breach in a timely manner so that appropriate action could be taken to minimize losses.

177. Fairbanks's duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to such risk, or defeats protections put in place to guard against that risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B.

178. Fairbanks had a duty to protect and safeguard the PHI/PII of Plaintiff and the Class from unauthorized access and disclosure. Additionally, Fairbanks owed Plaintiff and the Class a duty:

a. to exercise reasonable care in designing, implementing, maintaining, monitoring, and testing its networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' PHI/PII was adequately secured from impermissible release, disclosure, and publication;

b. to protect Plaintiff's and Class Members' PHI/PII by using reasonable and adequate data security practices and procedures;

c. to implement processes to quickly detect a data breach, security incident, or intrusion involving its networks and servers; and

d. to promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PHI/PII.

179. Fairbanks breached its duties, and thus was negligent, by failing to use reasonable measures to protect Plaintiff's and Class Members' PHI/PII.

180. The specific negligent acts and omissions committed by Fairbanks include, but are not limited to:

a. Failing to adopt, implement, and maintain adequate data security measures to safeguard Plaintiff's and Class Members' PHI/PII;

b. Failing to adequately monitor the security of its accounts, networks, and systems;

c. Failing to ensure its servers had plans in place to maintain reasonable data security safeguards;

d. Failing to implement and maintain adequate mitigation policies and procedures;

e. Allowing unauthorized access to Plaintiff's and Class Members' PHI/PII;

f. Failing to detect in a timely manner that Plaintiff's and Class Members' PHI/PII had been compromised; and

g. Failing to timely notify Plaintiff and Class Members about the Data Breach so they could take appropriate steps to mitigate the potential for identity theft and other damages.

181. Fairbanks's willful failure to abide by its duties to Plaintiff and Class Members was wrongful, reckless, and grossly negligent considering the foreseeable risks and known threats.

182. It was foreseeable that Fairbanks's failure to use reasonable measures to protect Plaintiff's and Class Members' PHI/PII would result in injury to Plaintiff and Class Members.

183. Furthermore, the breach of security was reasonably foreseeable given the known high frequency of cyberattacks and data breaches in the healthcare and tech industries.

184. As a direct and proximate result of Fairbanks's negligent conduct, including, but not limited to, its failure to implement and maintain reasonable data security practices and procedures as described above, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages (as alleged above).

185. Through Fairbanks's acts and omissions described herein, including but not limited to Fairbanks's failure to protect the PHI/PII of Plaintiff and Class Members from being stolen and misused, Fairbanks unlawfully breached its duty to use reasonable care to

adequately protect and secure the PHI/PII of Plaintiff and Class Members while it was within Fairbanks's possession and control.

186. Further, through its failure to provide timely and clear notification of the Data Breach to Plaintiff and Class Members, Fairbanks prevented Plaintiff and Class Members from taking meaningful, proactive steps to secure their PHI/PII and mitigate the impact of the Data Breach.

187. Plaintiff and Class Members could have taken actions earlier had they been timely notified of the Data Breach.

188. Plaintiff and Class Members could have enrolled in credit monitoring, medical monitoring, instituted credit freezes, and changed their passwords, among other things, had they been alerted to the Data Breach more quickly.

189. Plaintiff and Class Members suffered harm from Fairbanks's delay in notifying them of the Data Breach.

190. As a direct and proximate result of Fairbanks's conduct, including, but not limited to, Fairbanks's failure to implement and maintain reasonable data security practices and procedures, Plaintiff and Class Members have suffered or will suffer injury and damages, including, but not limited to: (i) the loss of the opportunity to determine for themselves how their PHI/PII is used; (ii) the publication and theft of their PHI/PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, medical theft, fraud, and/or unauthorized use of their PHI/PII, including the need for substantial credit monitoring and medical monitoring services for an extended period of time; (iv) lost time and opportunity costs associated with efforts expended to

address and mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest and recover from medical fraud and identity theft; (v) costs associated with placing freezes, reviewing medical statements, reviewing credit reports and changing passwords; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the continued risk to their PHI/PII, which remains in Fairbanks's possession and is subject to further unauthorized disclosures so long as Fairbanks fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the inevitable and continuing consequences of compromised PHI/PII for the rest of their lives. Thus, Plaintiff and the Class are entitled to damages in an amount to be proven at trial.

191. The damages Plaintiff and the Class have suffered and will suffer (as alleged above) were and are the direct and proximate result of Fairbanks's negligent conduct.

192. Plaintiff and the Class have suffered cognizable injuries and are entitled to actual and punitive damages in an amount to be proven at trial.

SECOND CAUSE OF ACTION
NEGLIGENCE *PER SE*
(Alleged Against Fairbanks on Behalf of Plaintiff and the Class)

193. Plaintiff re-alleges and incorporates all preceding paragraphs as though fully set forth herein.

194. Fairbanks had a duty to implement and maintain reasonable data security practices pursuant to Section 5 of the FTC Act, 15 U.S.C. § 45(a), which prohibits "unfair

. . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect sensitive and confidential data.

195. The FTC Act prohibits "unfair practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Fairbanks, for failing to use reasonable measures to protect PII/PHI/PII. The FTC publications and orders described above also formed part of the basis of Fairbanks's duty in this regard.

196. Fairbanks solicited, collected, stored, and maintained Plaintiff's and Class Members' PHI/PII as part of its regular business, which affects commerce.

197. Fairbanks violated the FTC Act by failing to use reasonable measures to protect Plaintiff's and Class Members' PHI/PII and by failing to comply with applicable industry standards, as described herein.

198. Fairbanks breached its duties to Plaintiff and the Class under the FTC Act by failing to implement and maintain fair, reasonable, and adequate data security practices to safeguard Plaintiff's and Class Members' PHI/PII, and by failing to provide prompt notice of the Data Breach without unreasonable delay.

199. Fairbanks's multiple failures to comply with applicable laws and regulations constitutes negligence *per se*.

200. Plaintiff and the Class are within the class of persons that the FTC Act was intended to protect.

201. The harm that occurred as a result of the Data Breach is the type of harm the

FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, like Fairbanks, that fail to employ reasonable data security measures and avoid unfair and deceptive practices, causing the same harm as that suffered by Plaintiff and the Class.

202. Fairbanks breached its duties to Plaintiff and the Class by unreasonably delaying and failing to provide notice of the Data Breach expeditiously and/or as soon as practicable to Plaintiff and the Class.

203. Fairbanks's violations of the FTC Act constitute negligence *per se*.

204. As a direct and proximate result of Fairbanks's negligence *per se*, Plaintiff and the Class have suffered, and continue to suffer, damages arising from the Data Breach, as alleged above.

205. The injury and harm that Plaintiff and Class members suffered (as alleged above) was the direct and proximate result of Fairbanks's negligence *per se*.

206. Fairbanks also had a duty to use reasonable security measures under HIPAA, which requires covered entities to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(1). Some or all of the medical information at issue in this action constitutes "protected health information" within the meaning of HIPAA.

207. Title II of HIPAA contains what are known as the Administrative Simplification provisions. 42 U.S.C. §§ 1301, *et seq*. These provisions require, among other things, that the Department of Health and Human Services ("HHS") create rules to

streamline the standards for handling PHI/PII. HHS subsequently promulgated multiple regulations under the authority of the Administrative Simplification provisions of HIPAA. These rules include 45 C.F.R. § 164.304, 45 C.F.R. § 164.306(a)(1-4), 45 C.F.R. § 164.312(a)(1), 45 C.F.R. § 164.308(a)(1)(i), 45 C.F.R. § 164.308(a)(1)(ii)(D), and 45 C.F.R. § 164.530(b).

208. Fairbanks's violations of HIPAA constitute negligence *per se*.

209. Plaintiff and the Class are within the class of persons HIPAA was intended to protect.

210. The harm that occurred as a result of the Data Breach is the type of harm HIPAA was intended to guard against.

211. Fairbanks's duty to use reasonable care in protecting Plaintiff's and Class Members' PHI/PII arose not only as a result of the statutes and regulations described above, but also because Fairbanks is bound by industry standards to protect and secure PHI/PII in its possession and control.

212. As a direct and proximate result of Fairbanks's negligence *per se*, Plaintiff and the Class have suffered and will suffer injury, including but not limited to: (i) actual instances of identity theft or fraud; (ii) the compromise, publication, and/or theft of their PHI/PII; (iii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PHI/PII; (iv) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, time and resources spent researching how to prevent, detect, contest, and recover from medical fraud and identity theft; (v) costs

associated with placing or removing freezes on credit reports; (vi) the continued risk to their PHI/PII, which remains in Fairbanks's possession and is subject to further unauthorized disclosures so long as Fairbanks fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the ongoing impact of the Data Breach for the remainder of the lives of Plaintiff and the Class.

213. Additionally, as a direct and proximate result of Fairbanks's negligence *per se*, Plaintiff and the Class have suffered and will suffer imminent and impending injuries arising from the increased risk of future fraud and identity theft.

214. As a direct and proximate result of Fairbanks's negligence *per se*, Plaintiff and the Class are entitled to recover actual, consequential, and nominal damages.

215. Plaintiff and the Class have suffered injury and are entitled to damages in amounts to be proven at trial.

THIRD CAUSE OF ACTION
BREACH OF IMPLIED CONTRACT
(Alleged Against Fairbanks on Behalf of Plaintiff and the Class)

216. Plaintiff re-alleges and incorporates all preceding paragraphs as though fully set forth herein.

217. Fairbanks solicited, collected, stored, and maintained Plaintiff's and Class Members' PHI/PII as part of Fairbanks's regular business practices.

218. Plaintiff and Class Members were required to provide their PHI/PII to Fairbanks to receive medical services. Plaintiff and Class Members paid money, or money was paid on their behalf, to Fairbanks in exchange for medical services.

219. Fairbanks solicited and accepted possession of Plaintiff's and Class Members' PHI/PII for the purpose of providing medical services to Plaintiff and Class Members.

220. In delivering, directly or indirectly, their PHI/PII to Fairbanks and paying for healthcare services, Plaintiff and Class Members intended and understood that Fairbanks would adequately safeguard their PHI/PII.

221. Plaintiff and Class Members reasonably expected that the PHI/PII they entrusted to Fairbanks, to receive medical services, would remain confidential and would not be shared or disclosed to criminal third parties or vendors with inadequate data security.

222. Plaintiff and Defendant had a mutual understanding that Fairbanks would ensure any third parties it hired, implemented and maintained adequate and reasonable data security practices and procedures to protect Plaintiff's and Class Members' sensitive PHI/PII.

223. Plaintiff and Fairbanks also shared an expectation and understanding that Fairbanks would not share or disclose, whether intentionally or unintentionally, the sensitive PHI/PII in its possession and control with third parties who had inadequate data security.

224. Based on Fairbanks's representations, legal obligations, and acceptance of Plaintiff's and Class Members' PHI/PII, Fairbanks had a duty to safeguard the PHI/PII in its possession by ensuring all vendors it utilized employed reasonable data security practices.

225. When Plaintiff and Class Members paid money and provided their PHI/PII

to Fairbanks, either directly or indirectly, in exchange for goods or services, they entered into implied contracts with Fairbanks.

226. Fairbanks entered into implied contracts with Plaintiff and the Class under which Fairbanks agreed to comply with its statutory and common law duties to safeguard and protect Plaintiff's and Class Members' PHI/PII and to timely notify Plaintiff and Class Members of a data breach.

227. The implied promise of confidentiality includes consideration beyond those pre-existing duties owed under HIPAA and other state and federal regulations.

228. The implied promises include, but are not limited to: (i) taking steps to ensure any agents or vendors who are granted access to PHI/PII protect the confidentiality of that information; (ii) taking steps to ensure that PHI/PII in the possession and control of Defendant, its agents, and/or vendors is restricted and limited to achieve an authorized medical purpose; (iii) restricting access to qualified and trained agents and/or vendors; (iv) designing and implementing appropriate retention policies to protect the PHI/PII from unauthorized access and disclosure; (v) applying or requiring proper encryption of the PHI/PII; (vi) requiring multifactor authentication for access to the PHI/PII; and (vii) other steps necessary to protect against foreseeable data breaches.

229. Plaintiff and Class Members would not have entrusted their PHI/PII to Fairbanks in the absence of such implied contracts.

230. Fairbanks knew that Plaintiff's and Class Members' PHI/PII is highly sensitive and must be protected, and that this protection was of material importance to Plaintiff and Class Members.

231. Plaintiff and Class Members fully performed their obligations under the implied contracts with Fairbanks.

232. Fairbanks breached the implied contracts with Plaintiff and Class Members by failing to safeguard Plaintiff's and Class Members' PHI/PII.

233. As a direct and proximate result of Fairbanks's breach of the implied contracts, Plaintiff and Class Members have suffered damages, including foreseeable consequential damages that Fairbanks knew about when it solicited and collected Plaintiff's and Class Members' PHI/PII.

234. Plaintiff and the Class have suffered injuries as described herein, and are entitled to actual and punitive damages, statutory damages, and reasonable attorneys' fees and costs, in an amount to be proven at trial.

FOURTH CAUSE OF ACTION
UNJUST ENRICHMENT
(Alleged Against Fairbanks on Behalf of Plaintiff and the Class)

235. Plaintiff re-alleges and incorporates all preceding paragraphs as though fully set forth herein.

236. Plaintiff alleges this claim in the alternative where necessary.

237. Plaintiff and the Class provided their PHI/PII to receive medical services.

238. By conferring their PHI/PII, Plaintiff and Class Members reasonably understood Fairbanks would be responsible for safeguarding their PHI/PII from unauthorized access and disclosure, including selecting vendors with adequate data security. Plaintiff also understood Fairbanks would responsibly safeguard and store their PHI/PII and employ adequate data security.

239. Upon information and belief, Fairbanks funds its data security measures entirely from its general revenue, including from money it from Plaintiff and Class Members.

240. Plaintiff and Class Members paid Fairbanks a certain sum of money, which was used to fund data security.

241. As such, a portion of the payments made by or on behalf of Plaintiff and the Class was to be used to provide a reasonable level of data security, and the amount of the portion of each payment made that is allocated to data security is known to Defendant.

242. There is a direct nexus between money paid to Defendant and the requirement that Defendant keep Plaintiff's and Class Members' PHI/PII confidential and protected from unauthorized access and disclosure.

243. Protecting the PHI/PII of Plaintiff and Class Members is integral to Defendant's business. Without their PHI/PII, Defendant would be unable to provide services comprising Defendant's core business.

244. Plaintiff's and Class Members' PHI/PII has monetary value.

245. Plaintiff and Class Members directly conferred a monetary benefit on Defendant. Plaintiff and Class Members directly conferred a monetary benefit on Fairbanks by supplying their PHI/PII, from which Fairbanks derives its business, and which should have been protected with adequate data security.

246. Defendant solicited, collected, stored, and maintained Plaintiff's and Class Members' PHI/PII, and as such, Defendant had direct knowledge of the monetary benefits

conferred upon them by Plaintiff and the Class. Defendant profited from these transactions and used Plaintiff's and Class Members' PHI/PII for business purposes.

247. Indeed, Plaintiff and Class Members who were patients of Fairbanks provided monetary payments to Fairbanks and therefore conferred a benefit unto Defendant.

248. Defendant appreciated that a monetary benefit was being conferred on it by Plaintiff and Class Members and accepted that monetary benefit.

249. Under the facts and circumstances outlined above, however, it is inequitable for Defendant to retain that benefit without payment of the value thereof.

250. Defendant enriched itself by saving the costs it reasonably should have expended on data security measures and vendors with adequate data security to secure Plaintiff's and Class Members' PHI/PII.

251. Instead of providing a reasonable level of security that would have prevented the Data Breach, Defendant calculated to increase its own profits at the expense of Plaintiff and Class Members by utilizing cheaper, ineffective security measures and vendors. Plaintiff and Class Members, on the other hand, suffered as a direct and proximate result of Defendant's decisions to prioritize its own profits over the requisite data security and vendors with requisite data security.

252. Under the principles of equity and good conscience, Defendant should not be permitted to retain the monetary benefit belonging to Plaintiff and Class Members, because Defendant failed to implement appropriate data management and security measures and/or failed to utilize vendors who implemented appropriate data management and security

measures.

253. Defendant acquired Plaintiff's and Class Members' PHI/PII through inequitable means. Fairbanks failed to disclose its inadequate data security practices.

254. If Plaintiff and Class Members knew that Defendant had not secured their PHI/PII, they would not have allowed Defendant to collect their PHI/PII.

255. Plaintiff and Class Members have no adequate remedy at law.

256. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered or will suffer injury, including, but not limited to: (i) actual identity theft and fraud; (ii) loss of the opportunity to control how their PHI/PII is used; (iii) the compromise, publication, and/or theft of their PHI/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, medical fraud, and/or unauthorized use of their PHI/PII; (v) lost time and opportunity costs associated with efforts to mitigate the actual and future consequences of the Data Breach, including, but not limited to, effort and time spent researching how to prevent, detect, contest, and recover from identity theft and medical fraud; (vi) the continued risk to their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession; and/or (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

257. As a direct and proximate result of Defendant's conduct, Plaintiff and Class Members have suffered and will continue to suffer other forms of injury and/or harm.

258. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiff and Class Members, all gains that they unjustly received.

FIFTH CAUSE OF ACTION
BREACH OF FIDUCIARY DUTY
(Alleged Against Fairbanks on Behalf of Plaintiff and the Class)

259. Plaintiff re-alleges and incorporates all preceding factual paragraphs as though fully set forth herein.

260. In light of the special relationship between Fairbanks, as a medical provider, and Plaintiff and Class Members, Fairbanks became a fiduciary by undertaking guardianship of Plaintiff's and Class Members' PHI/PII.

261. A physician has a fiduciary duty to not disclose a patient's medical information.

262. Fairbanks became a fiduciary, created by its undertaking and guardianship of Plaintiff's and the Class Members' PHI/PII, to act primarily for the benefit of Plaintiff and Class Members.

263. This duty included the obligation and responsibility to:

a. safeguard Plaintiff's and Class Members' PHI/PII;

b. timely notify Plaintiff and the Class in the event of a data breach;

c. only utilize vendors with adequate data security infrastructure, procedures, and protocols; and

d. establish and implement appropriate oversight and monitoring procedures for the activities of its vendors.

264. In order to provide Plaintiff and Class Members medical services, Fairbanks required that Plaintiff and Class Members provide their PHI/PII to Fairbanks.

265. Fairbanks knowingly undertook the responsibility and duties related to the possession of Plaintiff's and Class Members' PHI/PII, for the benefit of Plaintiff and Class Members and in order to provide Plaintiff and Class Members with medical services.

266. Fairbanks had a fiduciary duty to act for the benefit of Plaintiff and Class Members upon matters within the scope of its relationship with them.

267. Fairbanks breached the fiduciary duties it owed to Plaintiff and Class Members by failing to protect Plaintiff's and Class Members' PHI/PII by using a vendor with inadequate data security—Fairbanks.

268. Defendant further breached the fiduciary duties it owed to Plaintiff and Class Members by failing to timely notify and/or warn Plaintiff and Class Members of the Data Breach and by utilizing a vendor with inadequate data security infrastructure, procedures, and protocols.

269. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiff and Class Members have suffered or will suffer concrete injury, including, but not limited to: (i) actual misuse of their PHI/PII in the form of identity theft and fraud; (ii) the loss of the opportunity to control how their PHI/PII is used; (iii) the unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing of their PHI/PII; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, fraud, and/or unauthorized use of their PHI/PII; (v) lost opportunity costs associated with efforts to mitigate the actual and

future consequences of the Data Breach, including, but not limited to, time and effort spent researching how to prevent, detect, contest, and recover from identity theft; (vi) the continued risk to their PHI/PII, which remains in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI/PII in its continued possession; and (vii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the Data Breach for the remainder of the lives of Plaintiff and Class Members.

270. As a direct and proximate result of Defendant's breach of its fiduciary duties, Plaintiff and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

SIXTH CAUSE OF ACTION
DECLARATORY AND INJUNCTIVE RELIEF
(Alleged Against Fairbanks on Behalf of Plaintiff and the Class)

271. Plaintiff re-alleges and incorporates all preceding paragraphs as though fully set forth herein.

272. Fairbanks owed and still owes a duty of care to Plaintiff and Class Members that requires it to adequately secure Plaintiff's and Class Members' PHI/PII.

273. Upon information and belief, Fairbanks still possesses Plaintiff's and Class Members' PHI/PII.

274. Fairbanks has not satisfied its legal duties to Plaintiff and Class Members.

275. Since the Data Breach, Fairbanks has not announced any changes to its data security infrastructure, processes or procedures to fix the vulnerabilities in its computer

systems and/or security practices which permitted the Data Breach to occur and go undetected and, thereby, prevent further attacks.

276. Fairbanks has not satisfied its legal duties to Plaintiff and the Class. In fact, now that Fairbanks's insufficient data security is known to hackers, the PHI/PII in Fairbanks's possession is even more vulnerable to cyberattacks.

277. Further, Plaintiff and Class Members are at risk of additional or further harm due to the exposure of their PHI/PII and Fairbanks's failure to address the security failings that led to such exposure.

278. There is no reason to believe that Fairbanks's data security measures are any more adequate now than they were before the Data Breach.

279. Plaintiff and the Class, therefore, seek a declaration (1) that Fairbanks's existing security measures do not comply with its obligations and duties of care to provide adequate security, and (2) that to comply with its obligations and duties of care, Fairbanks must implement and maintain reasonable security measures, including, but not limited to:

a. Ordering that Fairbanks engage third-party security auditors and penetration testers, as well as internal security personnel, to conduct testing, including simulated attacks, penetration tests, and audits on Fairbanks's systems on a periodic basis, and ordering Fairbanks to promptly correct any problems or issues detected by such third-party security auditors;

b. Ordering that Fairbanks engage third-party security auditors and internal personnel to run automated security monitoring;

c. Ordering that Fairbanks audit, test, and train its security personnel regarding

any new or modified procedures;

d. Ordering that Fairbanks segment data by, among other things, creating firewalls and access controls so that if one area of Fairbanks's systems is compromised, hackers cannot gain access to other portions of Fairbanks's systems;

e. Ordering that Fairbanks purge, delete, and destroy, in a reasonably secure manner, customer data not necessary for their provisions of services;

f. Ordering that Fairbanks conduct regular database scanning and security checks; and

g. Ordering that Fairbanks routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendant as follows:

a. For an order certifying this action as a Class Action, defining the Class as requested herein, appointing the undersigned as Class counsel, and finding that Plaintiff are proper representatives of the Class requested herein;

b. For a judgment in favor of Plaintiff and the Class, awarding them appropriate monetary relief, including compensatory damages, punitive damages, nominal damages, attorneys' fees, expenses, costs, and such other and further relief as is just and proper;

c. For an order providing injunctive and other equitable relief as necessary to protect the interests of the Class as requested herein;

d. For an order requiring Defendant to pay the costs involved in notifying the Class about the judgment and administering the claims process;

e. For a judgment in favor of Plaintiff and the Class, awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs, and expenses as allowable by law; and

f. For an award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff hereby demands a trial by jury on any and all issues raised in this Class Action Complaint so triable as of right.

Date: July 15, 2025

Respectfully Submitted,

By: */s/ Joshua Cooley*

Joshua B. Cooley, 1409065
Katherine Elsner, 1411116
EHRHARDT, ELSNER & COOLEY
215 Fidalgo Ave, Suite 201
Kenai AK 99611
Phone: (907) 283-2876
Facsimile: (907) 283-2896
Email: josh@907legal.com
Email : katie@907legal.com

William B. Federman
(*pro hac vice* anticipated)
FEDERMAN & SHERWOOD
10205 North Pennsylvania Avenue
Oklahoma City, OK 73120
Phone: (405) 235-1560
Email: wbf@federmanlaw.com